



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/588,787	08/09/2006	Wataru Matsumoto	2611-0260PUS1	2763
2292	7590	01/26/2009	EXAMINER	
BIRCH STEWART KOLASCH & BIRCH			ALPHONSE, FRITZ	
PO BOX 747			ART UNIT	PAPER NUMBER
FALLS CHURCH, VA 22040-0747			2112	
NOTIFICATION DATE	DELIVERY MODE			
01/26/2009	ELECTRONIC			

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No.	Applicant(s)
	10/588,787	MATSUMOTO, WATARU
	Examiner	Art Unit
	FRITZ ALPHONSE	2112

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 2 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 09 August 2006.
 2a) This action is **FINAL**. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 8-16 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) 8-16 is/are allowed.
 6) Claim(s) _____ is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 8/09/2006 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date 3, 15, 16, 29.

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____.
 5) Notice of Informal Patent Application
 6) Other: _____.

Quayle Action

DETAILED ACTION

1. This Office Action is in regard to the Preliminary Amendment filed on 8/09/2006.

Claims 1-7 are canceled, claims 8-16 are pending.

Information Disclosure Statement

2. The Information Disclosure Statement (IDS) submitted is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement has been considered by the examiner.

Oath/Declaration

3. The Oath/Declaration filed 8/09/2006 is accepted.

4. This application is in condition for allowance except for the following formal matters:

5. The drawings filed 8/09/2006 are objected to because:

Figure 19 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

6. Claim 8 is objected to because of the following informalities: it is not clear if the phrases "error-correction-information" in line 5 and "error correction information" in lines 7 or 15 of the claim have the same meaning. Appropriate correction is required. Prosecution on the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

A shortened statutory period for reply to this action is set to expire **TWO MONTHS** from the mailing date of this letter.

Allowable Subject Matter

7. After further search and thorough examination of the present application and in view of the prior art of record, claims 8-16 are found to be in condition for allowance.

Reason for Allowance

8. The following is an examiner's statement of reasons for allowance: The present invention relates to a quantum key distribution method capable of correcting a data error using an error correction code and a communication apparatus capable of realizing the quantum key distribution.

To achieve this inventive goal, independent claim 8 identifies the distinct features "the transmission-side communication apparatus notifying the reception-side communication apparatus of additional second error correction information generated based on a third parity check matrix and the transmission data, via the public communication path, the third parity check matrix, which is identical in both of the communication apparatuses, corresponding to a coding rate lower than a last coding rate, and being extracted, when the error of the reception data is not completely corrected,

from the first parity check matrix such that last error correction information becomes a part of information at a time of next error correction; second error correcting including the reception-side communication apparatus correcting the error of the reception data based on the first error correction information and the second error correction information; and encryption-key generating including, when the error of the reception data is completely corrected at the first error correcting or when the error is completely corrected by repeatedly executing the second check-matrix generating, the second error-correction-information notifying, and the second error correcting, discarding a part of shared information according to an amount of opened error correction information; and setting a result of the discarding as an encryption key.”

Independent claim 13 identifies the distinct features “an encryption-key generating unit that discards a part of the shared information according to an amount of opened error correction information and sets a result of discarding as an encryption key, when the error of the reception data is completely corrected, wherein the decoding unit corrects the error of the reception data based on a third parity check matrix and error correction information added from the transmission-side communication apparatus via the public communication path, the third parity check matrix, which is identical in both of the communication apparatuses, corresponding to each coding rate, and being extracted, when the error of the reception data is not completely corrected, from the first parity check matrix such that last error correction information becomes a part of information at a time of next error correction while decreasing the coding rate.”

Independent claim 15 identifies the distinct features “an encryption-key generating unit that discards a part of the shared information according to an amount of

opened error correction information and sets a result of discarding as an encryption key, when the error of the reception data is completely corrected, wherein the error-correction-information generating unit notifies the reception-side communication apparatus of additional error correction information via the public communication path until the error of the reception data is completely corrected, based on a third parity check matrix, which is identical in both of the communication apparatuses, corresponding to each coding rate, the third parity check matrix being extracted, when the error of the reception data is not completely corrected, from the first parity check matrix such that last error correction information becomes a part of information at a time of next error correction while decreasing the coding rate.”

The first cited reference, Nambu (U.S. Pat. No. 6,801,626) discloses a cryptographic key distribution using light pulses of three macroscopic quantum states. The second cited reference Townsend (U.S. Pat. No. 5,768,378) discloses a key distribution in a multiple access network using quantum cryptography.

However, the features disclosed in the instant application (No. 10/588,787) are neither anticipated nor render obvious by the prior art of record.

These limitations, in conjunction with all other limitations of the base claims were not shown by, would not have been obvious over, would not have been fairly suggested by the prior art of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fritz Alphonse, whose telephone number is (571) 272-3813. The examiner can normally be reached on M-F, 8:30-6:00, Alt. Mondays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Scott Baderman, can be reached at (571) 272-3644.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (571) 272-3824

Information regarding the status of an application may also be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/FA/

Examiner, Art Unit 2112

January 14, 2009

/Esaw T Abraham/

Primary Examiner, Art Unit 2112